Identity Theft

Credential attacks

You can split credential-targeting attacks into several categories:

- Offline attacks (recovering a user's password from captured authentication data)
- Passive online attacks (intercepting authentication data and using it to crack passwords or spoof an authorised user). While eavesdropping and password cracking is time-consuming and hard to detect, Man-in-the-Middle attacks and replay attacks are very effective as they don't require attackers to crack a password
- Active online attacks (guessing passwords). Guessing a password by repeatedly trying different combinations at logon is both slow and easy to detect. More importantly, only weak passwords are vulnerable to this attack
- Non-technological attacks

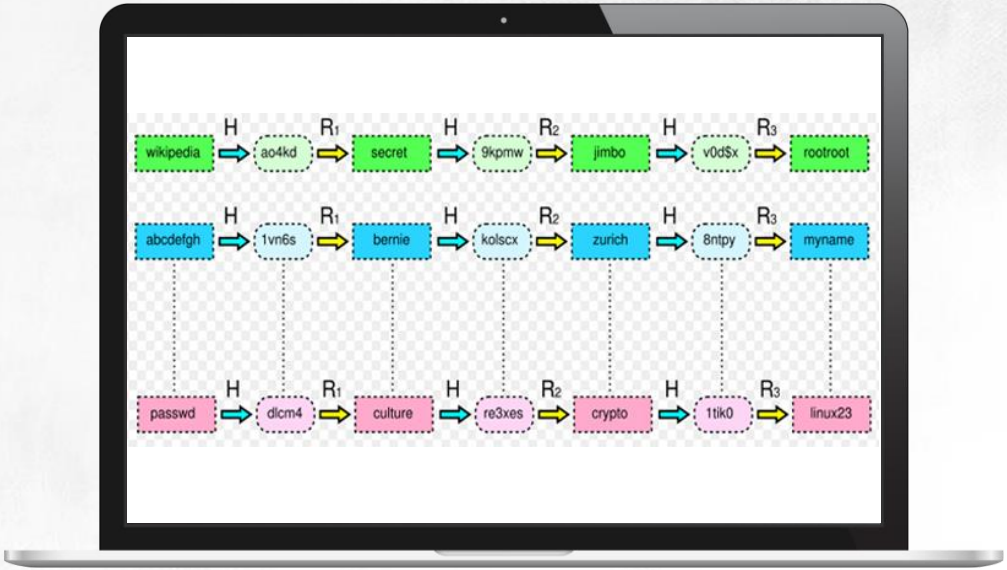
Offline Attacks

Rainbow tables

Seeing as brute-force is inefficient and time-consuming, it can be sped up if you pre-compute a database of all possible hashes

This solution would require a large hash database:

- LM hash values storage takes 310 TB
- Storage for shorter than 15 characters NT hashes takes 5,652,897,009 Exabytes

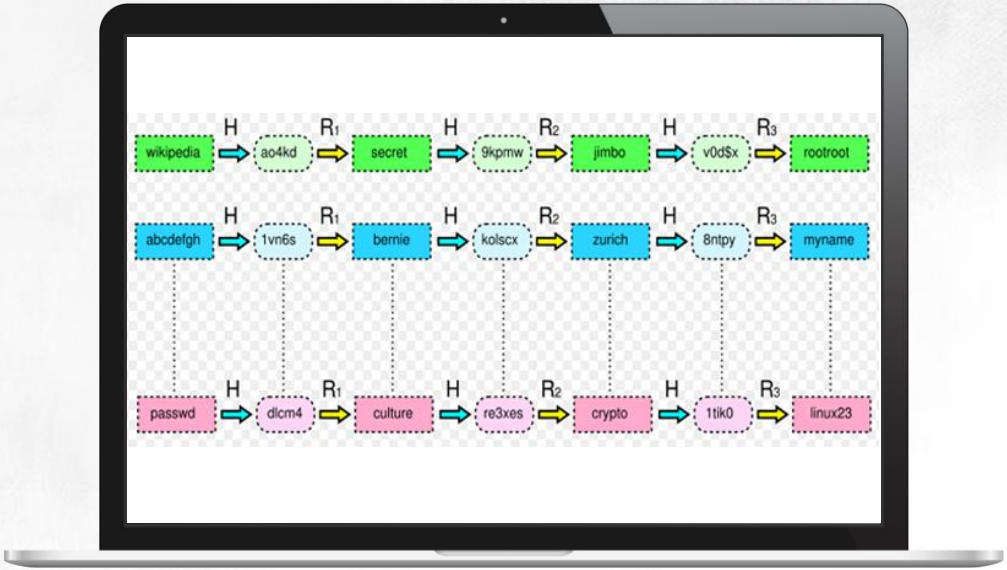


Offline Attacks

Rainbow tables

Developed by Philippe Oechslin, the rainbow tables are a combination of both these techniques

Rather than include all possible hashes, the rainbow tables only contain some passwords and hashes for them

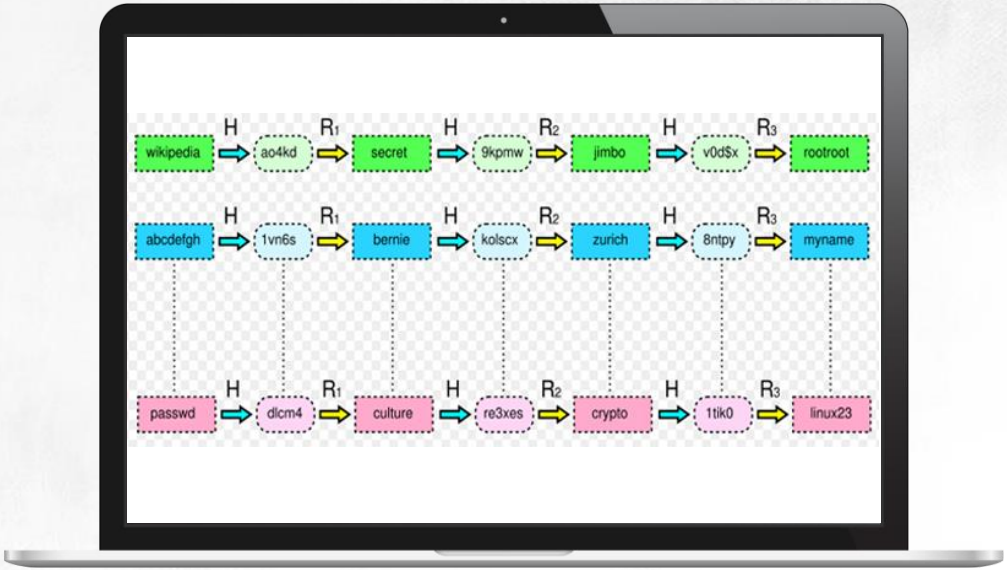


Offline Attacks

Rainbow tables

The trick lies in using a reduction function, a function that associates a hash with a corresponding password. It is the opposite of a hash function

Rainbow tables only contain first passwords of a chain and their last hashes

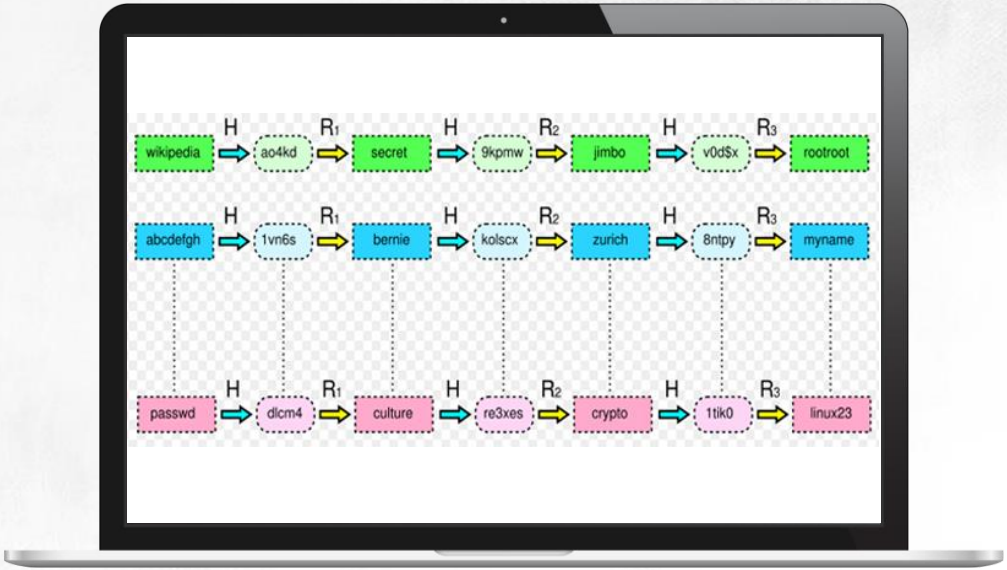


Offline Attacks

Rainbow tables

To check if the hash you have comes from any of the passwords in a given chain, you need to transform it using a reduction function (getting new passwords) and then calculate the hashes of these passwords

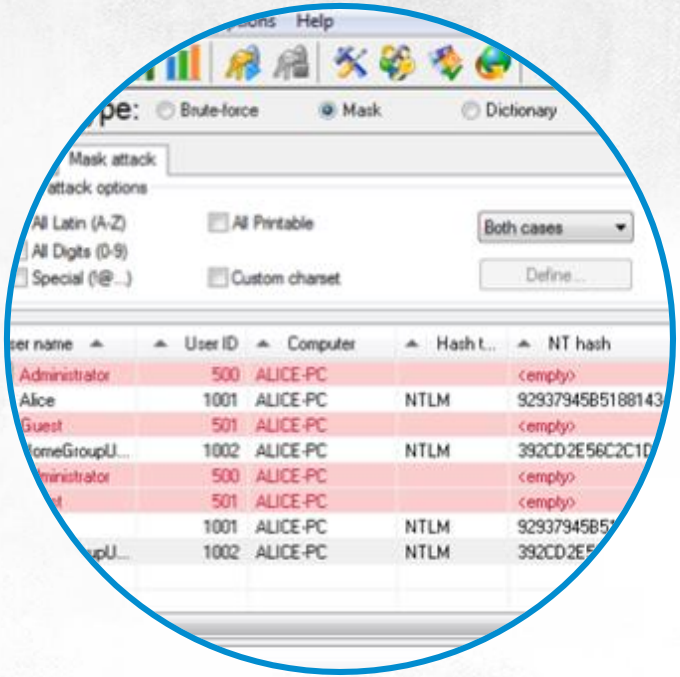
If the hash you obtain matches the credentials you got, the last password generated using reduction functions is the user password you seek



Exercise

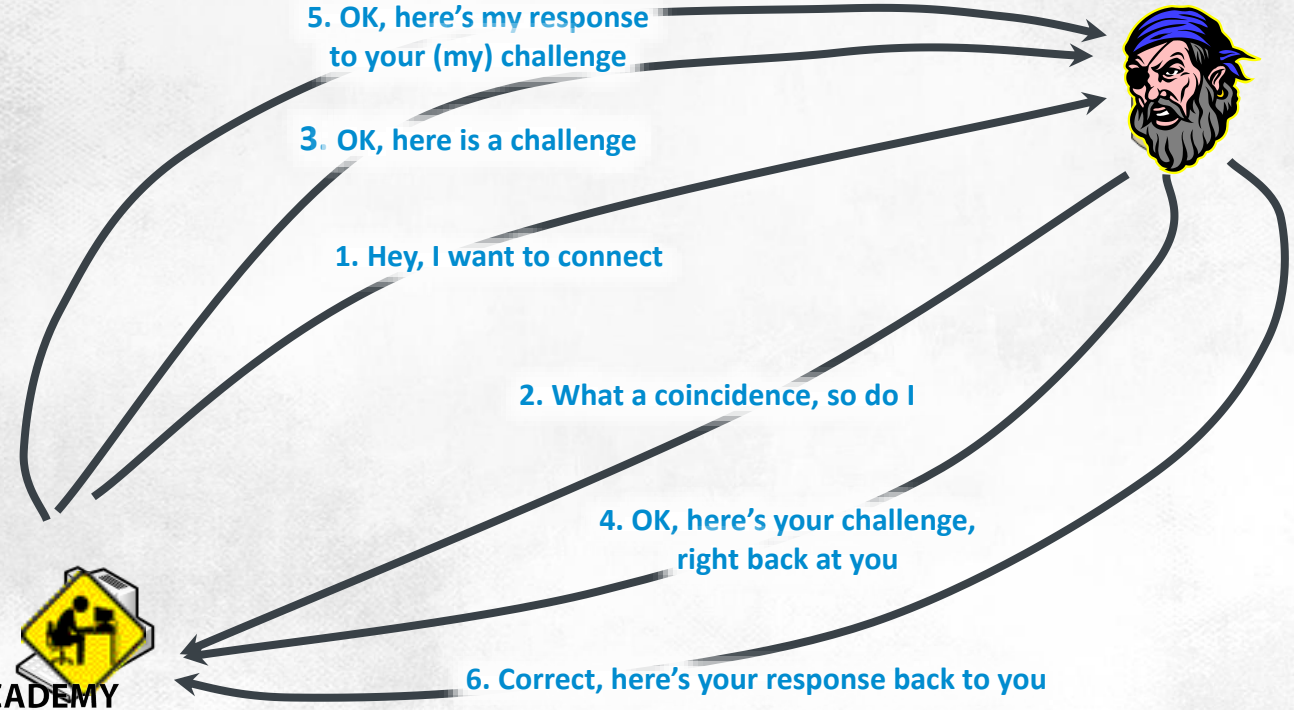
Offline attacks

- Cracking LM and NT hashes using ophcrack launched on a targeted computer
- Cracking LM and NT hashes using ophcrack launched on the attacker's computer
- Recovering a password from an NT hash and a cracked LM hash
- Cracking LM and NT hashes using an online service



Passive online attacks

Replay attack


5. OK, here's my response to your (my) challenge
3. OK, here is a challenge
1. Hey, I want to connect
2. What a coincidence, so do I
4. OK, here's your challenge, right back at you
6. Correct, here's your response back to you

Passive online attacks

The LM and NTLM protocols (and others) are vulnerable to replay attacks

The protective measure against replay attacks is signing all transmitted data packets

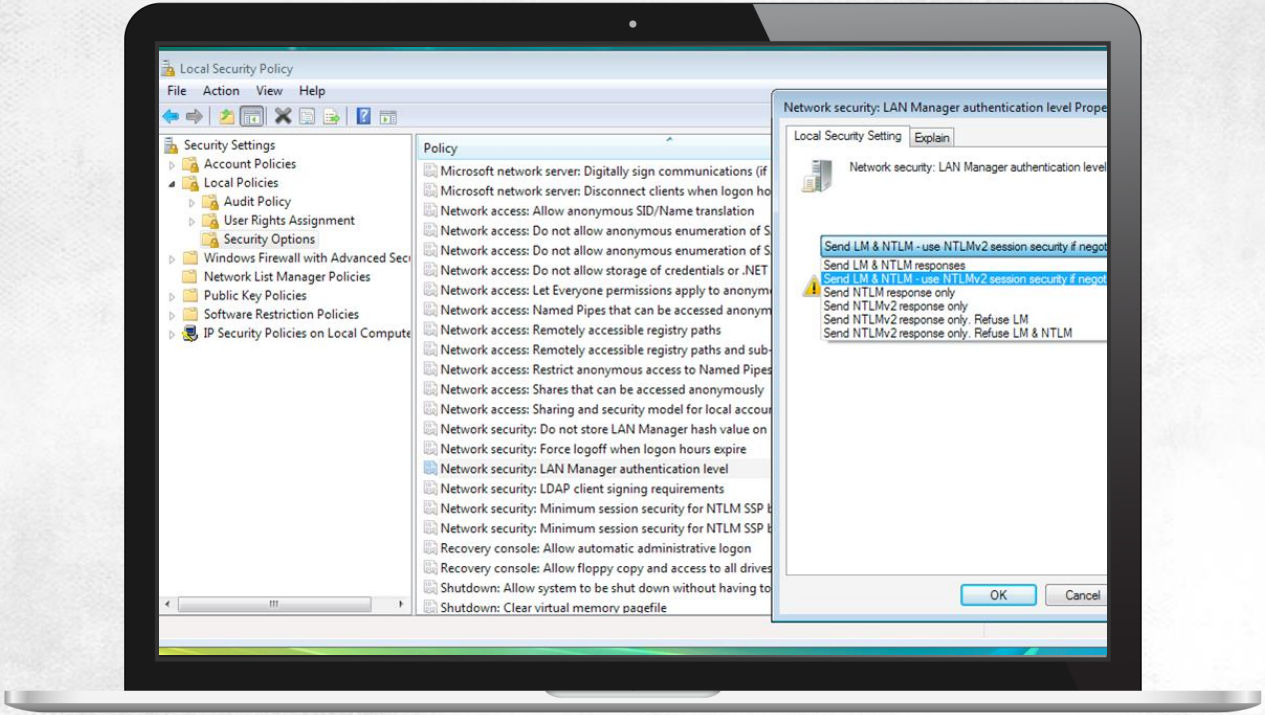
To do this, check Digitally sign communications (always) found here: Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options/Microsoft Network Server

Challenge/response message attacks: since the first 8 bytes of an LM hash are computed based on the first seven letters of the hash, and the second 8 bytes are computed based on letters 8 to 14, and since the user password is not modified in any way before it is split, it's easy to determine the plaintext

To protect yourself against challenge/response attacks, block LM authentication and NTLM v1 authentication. To do this, configure the Network Security: LAN Manager authentication level local policy

Passive online attacks

Protection


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
IP Security Policies on Local Compute
Policy
Microsoft network server: Digitally sign communications (if
Microsoft network server: Disconnect clients when logon ho
Network access: Allow anonymous SID/Name translation
Network access: Do not allow anonymous enumeration of S
Network access: Do not allow anonymous enumeration of S
Network access: Do not allow storage of credentials or .NET
Network access: Let Everyone permissions apply to anonym
Network access: Named Pipes that can be accessed anonym
Network access: Remotely accessible registry paths
Network access: Remotely accessible registry paths and sub
Network access: Restrict anonymous access to Named Pipes
Network access: Shares that can be accessed anonymously
Network access: Sharing and security model for local accou
Network security: Do not store LAN Manager hash value on
Network security: Force logoff when logon hours expire
Network security: LAN Manager authentication level
Network security: LDAP client signing requirements
Network security: Minimum session security for NTLM SSP
Network security: Minimum session security for NTLM SSP
Recovery console: Allow automatic administrative logon
Recovery console: Allow floppy copy and access to all drives
Shutdown: Allow system to be shut down without having to
Shutdown: Clear virtual memory pagefile
Network security: LAN Manager authentication level Prope
Local Security Setting
Explain
Network security: LAN Manager authentication level
Send LM & NTLM - use NTLMv2 session security if negot
Send LM & NTLM responses
Send LM & NTLM - use NTLMv2 session security if negot
Send NTLM response only
Send NTLMv2 response only
Send NTLMv2 response only. Refuse LM
Send NTLMv2 response only. Refuse LM & NTLM
OK
Cancel

Passive online attacks

Kerberos is not immune to long-term key guessing attacks (which RFC1510 admits). They are possible to perpetrate if attackers have good comparison resources

They can obtain this data by for example intercepting the KRB_AS_REQ message

Because the timestamp in this message is encrypted with a user's long-term key, if they are able to get data in the yyyymmddhhmmssZ format, they have practically cracked the key

The only way to protect from these attacks, apart from using smart cards, is to force users to set long and complex passwords and change them regularly

Passive online attacks

```
C:\>kerbsniff  keys
KerbSniff 1.2 - (c) 2002, Arne Vidstrom
          - http://ntsecurity.nu/toolbox/kerbcrack/
Captured packets: **

testkrb
INTRANET
27312F3871E385742E4B778223CAF8127A2D3D4
F4C7D548305E9DB69DD83B6B0A8E6A43E33C0D
8449A4BEDB36DFC7CC28EA8A92D
#
```

```
C:\>kerbcrack.exe keys -d dictionary.lst
KerbCrack 1.2 - (c) 2002, Arne Vidstrom
          - http://ntsecurity.nu/toolbox/kerbcrack/
Loaded capture file.
Currently working on:
 Account name    - testkrb
 From domain     - INTRANET
 Trying password - Tajne-Hasl0
Number of cracked passwords this far: 2
```

THANKS